NOTE ON VANISHING POWER SUMS OF ROOTS OF UNITY

NEERAJ KUMAR AND K. SENTHIL KUMAR

Abstract. For fixed positive integers m and ℓ, we give a complete list of integers n for which their exist mth complex roots of unity $x_1, \ldots, x_n$ such that $x_1^\ell + \cdots + x_n^\ell = 0$. This extends the earlier result of Lam and Leung on vanishing sums of roots of unity. Furthermore, we characterize all positive integers n with $2 \leq n \leq m$, for which there are distinct mth complex roots of unity $x_1, \ldots, x_n$ such that $x_1^\ell + \cdots + x_n^\ell = 0$.

1. Introduction

Let m be a positive integer. By an mth root of unity, we mean a complex number ζ such that $\zeta^m = 1$. That is, a root of the polynomial $X^m - 1$. One can easily see that the roots of $X^m - 1$ are distinct, in fact there are exactly m, mth roots of unity. Using the relationship between the roots and the coefficients of a polynomial, we see that the sum of all mth roots of unity, which is the coefficient of X^{m-1} in $X^m - 1$, is zero. A natural question is: What are all the positive integers n for which there exist mth roots of unity $x_1, \ldots, x_n$ (repetition is allowed) such that $x_1 + \cdots + x_n = 0$. A beautiful result of T. Y. Lam and K. H. Leung [1] gives a complete classification of all such integers. Suppose m has prime factorization $p_1^{a_1} \ldots p_r^{a_r}$, where $a_i > 0$, then we have the following theorem due to Lam and Leung:

Theorem 1. *Let n be a positive integer. Then there are mth roots of unity $x_1, \ldots, x_n$ such that $x_1 + \cdots + x_n = 0$ if and only if n is of the form $n_1p_1 + \cdots + n_rp_r$ where each n_i is a non-negative integer for $1 \leq i \leq r$.*

Theorem 1 motivate us to ask the following:

Question 1. *Let m and ℓ be positive integers. What are all the positive integers n for which there exist mth roots of unity $x_1, \ldots, x_n$ such that $x_1^\ell + \cdots + x_n^\ell = 0$?*

Note that when $\ell = 1$, the complete answer to Question 1 is given by Theorem 1. However, for $\ell \geq 2$, we do not find any results in this direction in the literature. Our objective here is to study the case when $\ell \geq 2$. First, we fix some notations.

Date: Submitted: March 30, 2015, Revision submitted: May 04, 2015.

Key words: roots of unity, power sum.

2000 Mathematics Subject Classification: Primary 11L03 Secondary 11R18.

Let m be a positive integer, and let Ω_m denotes the set of all mth roots of unity. For a positive integer ℓ, $W_\ell(m)$ denotes the set of all positive integers n for which there exist n-elements $x_1, \ldots, x_n \in \Omega_m$ such that $x_1^\ell + \cdots + x_n^\ell = 0$. When $\ell = 1$, we simply denote $W_\ell(m)$ by $W(m)$. With this notation, Question 1 can be reformulated as follows: *Let m and ℓ be positive integers. What are all the positive integers in the set $W_\ell(m)$?*

It is clear that if m divides ℓ then $W_\ell(m)$ is an empty set. Suppose that there are mth complex roots of unity, say, $x_1, \ldots, x_n$ such that $x_1^\ell + \cdots + x_n^\ell = 0$. Since the ℓth power of an mth root of unity is still an mth root of unity, the equation $x_1^\ell + \cdots + x_n^\ell = 0$ with $x_i \in \Omega_m$ can be written in the form $y_1 + \cdots + y_n = 0$ with $y_i \in \Omega_m$. This shows that for any positive integer m and ℓ, $W_\ell(m)$ is a subset of $W(m)$. It follows from Theorem 1 that any positive integers in the set $W_\ell(m)$ must be of the form $n_1 p_1 + \cdots + n_r p_r$ where each n_i is a non-negative integer for $1 \leq i \leq r$. In Section 2, we give a complete list of integers in the set $W_\ell(m)$ (see Theorem 2). Moreover, in Section 3 we find all positive integers $n \in W_\ell(m)$ for which there are distinct mth complex roots of unity $x_1, \ldots, x_n$ such that $x_1^\ell + \cdots + x_n^\ell = 0$ (see Theorem 3).

There are algebraic aspects why Question 1 is important. For instance, for a positive integer a, denote by p_a the power sum polynomial $X_1^a + \cdots + X_n^a$ of degree a. Let $\ell < k$ be two positive integers. In commutative algebra, one encounters the following situation: To show that the ideal $\langle p_\ell, p_k \rangle$ generated by the polynomials p_ℓ and p_k is a prime ideal in $\mathbb{C}[X_1, \ldots, X_n]$, one needs to show that the power sum polynomial $X_1^\ell + \cdots + X_n^\ell$ does not vanish when one allows the X_i's to take values among the $(\ell - k)$th roots of unity [2, see proof of Theorem 3.8].

Acknowledgment: We are grateful to Professor Ram Murty for his valuable suggestions regarding the paper. We also thank the referee for many useful comments for improving the manuscript. This project was funded by the Department of Atomic Energy (DAE), Government of India.

2. VANISHING OF POWER SUMS OF ROOTS OF UNITY

Let m and ℓ be positive integers. In this section, we completely characterize all the positive integers in the set $W_\ell(m)$. More precisely, we prove the following theorem:

Theorem 2. *Let m and ℓ be positive integers. Let $d = (m, \ell)$ be the greatest common divisor of m and ℓ. Then $W_\ell(m) = W(m/d)$.*

In other words, Theorem 2 says that: For any positive integer n, $x_1^\ell + \cdots + x_n^\ell = 0$ with $x_i \in \Omega_m$ if and only if $y_1 + \cdots + y_n = 0$ with $y_i \in \Omega_{m/d}$.

Proof. It is well known that Ω_m, that is, the set of all mth roots of unity, form a group with respect to the multiplication of complex numbers. In fact, it is a cyclic group of order m, generated by the complex number $\zeta_m = \cos 2\pi/m + \mathfrak{i}\sin 2\pi/m$. There is a remarkable property about finite cyclic groups. Namely, if G is a finite cyclic group and l is a positive integer relatively prime to the order of G, then the map

$$x \longmapsto x^{\ell} \quad (x \in G) \tag{1}$$

is an automorphism of G (In fact, all the automorphisms of G are of the form (1) for some integer ℓ which is relatively prime to the order of G). It follows that, if ℓ is a positive integer which is relatively prime to m then every element of Ω_m is a ℓth power of some element of Ω_m. Thus, for an integer l which is relatively prime to m, the equation $x_1^{\ell} + \cdots + x_n^{\ell} = 0$ with $x_i \in \Omega_m$ can be replaced by $y_1 + \ldots + y_n = 0$ with $y_i \in \Omega_m$, and vice versa. This discussion proves Theorem 2 for the case when ℓ is relatively prime to m.

Now assume that $d > 1$. Consider the map

$$\psi_d : \Omega_m \longrightarrow \Omega_{m/d} \tag{2}$$

defined by $x \mapsto x^d$ for $x \in \Omega_m$. This map is clearly onto, and the kernel is exactly Ω_d. Thus, $\Omega_m/\Omega_d \cong \Omega_{m/d}$. Now suppose that there are elements $x_1, \ldots, x_n \in \Omega_m$ such that $x_1^{\ell} + \cdots + x_n^{\ell} = 0$. Then this sum can be rewritten as $\left(x_1^{\ell/d}\right)^d + \cdots + \left(x_n^{\ell/d}\right)^d = 0$. Since ℓ/d and m are relatively prime, by the above discussion, the latter equation can be rewritten in the form $y_1^d + \cdots + y_n^d = 0$ with $y_i \in \Omega_m$. Finally, using the map ψ_d, the latter sum can be realized as $z_1 + \ldots + z_n = 0$ where $z_i \in \Omega_{m/d}$ for $1 \leq i \leq n$. In fact, all these steps can be reversed. This completes the proof of Theorem 2. $\square$

Combining Theorems 1 and 2, we have the following corollary:

Corollary 1. *Let m, n and ℓ be positive integers. Let $d = (m, \ell)$ be the greatest common divisor of m and ℓ. Then there are mth roots of unity $x_1, \ldots, x_n$ such that $x_1^{\ell} + \cdots + x_n^{\ell} = 0$ if and only if n is of the form $n_1q_1 + \cdots + n_sq_s$ where each n_i is a non-negative integer for $1 \leq i \leq s$ and $q_1, \ldots, q_s$ are distinct prime divisors of m/d.*

Example. Let $m = 60$, and let ℓ be an integer with $1 \leq \ell < 60$. By Theorem 2, $W_{\ell}(m) = W(m/d)$ where d is the greatest common divisor of m and ℓ. When d varies over the divisors of m, m/d also varies over the divisors of m. Thus $W_{\ell}(m)$ coincides with $W(d)$ for some divisor d of m. On the other hand, by Theorem 1, $W(d) = \sum_{i=1}^{s} q_i\mathbb{N}$ where $d = q_1^{b_1} \ldots q_s^{b_s}$ is the prime factorization of d. Here $\mathbb{N}$

denotes the set of non-negative integers. We thus have the following table which describe $W(d)$ for all positive divisors d of $m = 60$.

d	$W(d)$
1	$\emptyset$
2	$2\mathbb{N}$
3	$3\mathbb{N}$
4	$2\mathbb{N}$
5	$5\mathbb{N}$
6	$2\mathbb{N} + 3\mathbb{N} = \mathbb{N} \setminus \{1\}$
10	$2\mathbb{N} + 5\mathbb{N} = \mathbb{N} \setminus \{1, 3\}$
12	$2\mathbb{N} + 3\mathbb{N} = \mathbb{N} \setminus \{1\}$
15	$3\mathbb{N} + 5\mathbb{N} = \mathbb{N} \setminus \{1, 2, 4, 7\}$
20	$2\mathbb{N} + 5\mathbb{N} = \mathbb{N} \setminus \{1, 3\}$
30	$2\mathbb{N} + 3\mathbb{N} + 5\mathbb{N} = \mathbb{N} \setminus \{1\}$
60	$2\mathbb{N} + 3\mathbb{N} + 5\mathbb{N} = \mathbb{N} \setminus \{1\}$

3. Vanishing of power sums of distinct roots of unity

Let m and ℓ be two positive integers. For an integer $n \in W_\ell(m)$, the *height* $H(n; \ell, m)$ of n is defined to be the smallest positive integer h for which there are mth roots of unity $x_1, \dots, x_n$ such that $x_1^\ell + \cdots + x_n^\ell = 0$ and the maximum among the repetition of x_i's is h, that is, h is the maximum among the h_i, where h_i is the number of times x_i appears in the list $x_1, \dots, x_n$. When $\ell = 1$, we denote $H(n; \ell, m)$ by $H(n; m)$. Note that $H(n; m) = 1$ provided $2 \le n \le m$. Gary Sivek [3] refined the work of Lam and Leung by proving that for any integers $m \ge 2$ and $2 \le n \le m$, $H(n; m) = 1$ if and only if both n and $m - n$ are expressible as a linear combination of the prime factors of m with non-negative integer coefficients. Here we extend Sivek's result to vanishing of power sums of distinct roots of unity:

Theorem 3. *Let m and l be positive integers, and let n be an integer such that $2 \le n \le m$. Let d be the greatest common divisor of m and ℓ. Then $H(n; \ell, m) = 1$ if and only if $H(n; m/d) \le d$.*

Proof. Let $\Omega_{m/d} = \{z_1, \dots, z_{m/d}\}$. Suppose that there are distinct mth roots of unity $x_1, \dots, x_n$ such that $x_1^\ell + \cdots + x_n^\ell = 0$. Since d is the greatest common divisor of ℓ and m, this equation can be rewritten in the form $y_1^d + \cdots + y_n^d = 0$ with $y_1, \dots, y_n$ are mth roots of unity. Using the map ψ_d, the latter equation can be written as $\sum_{i=1}^{m/d} a_i z_i = 0$ where a_i is the cardinality of the set $\{y_1, \dots, y_n\} \cap \psi_d^{-1}(z_i)$ for $1 \le i \le m/d$. On the other hand, $\psi_d^{-1}(z)$ has exactly d elements for each $z \in \Omega_{m/d}$. It follows that $H(n; m/d) \le \max\{a_1, \dots, a_{m/d}\} \le d$. This proves that if $H(n; \ell, m) = 1$ then $H(n; m/d) \le d$.

Conversely, suppose that $H(n; m/d) \leq d$. Then there is a partition $(a_1, \ldots, a_{m/d})$ of n into non-negative integers a_i with $a_i \leq d$ for $1 \leq i \leq m/d$ and $\sum_{i=1}^{m/d} a_i z_i = 0$. Let y_i be any element of $\psi_d^{-1}(z_i)$ for $1 \leq i \leq m/d$. Then $\psi_d^{-1}(z_i) = y_i \Omega_d = \{ y_i x \mid x \in \Omega_d\}$. Since $a_i \leq d$, one can replace $a_i z_i$ by $y_i^d(x_1^d + \cdots + x_{a_i}^d)$ where $x_1, \ldots, x_{a_i}$ are distinct elements of Ω_d. Hence $H(n; \ell, m) = H(n; d, m) = 1$ since $\sum_{i=1}^{m/d} a_i = n$. This completes the proof of Theorem 3. $\square$

References

[1] T. Y. Lam and K. H. Leung: *On Vanishing sums of roots of unity.* J. Algebra **224** (2000), no. 1, 91–109.

[2] Neeraj Kumar: *Prime ideals and regular sequences of symmetric polynomials.* arXiv:1309.1098[math.AC].

[3] G. Sivek: *On vanishing sums of distinct roots of unity* Integers, **10** (2010), pp. A31, 365–368.

The Institute of Mathematical Sciences, 4th cross road, CIT Campus, Taramani, Chennai 600113, India

E-mail address: neerajkr@imsc.res.in, senthilkk@imsc.res.in